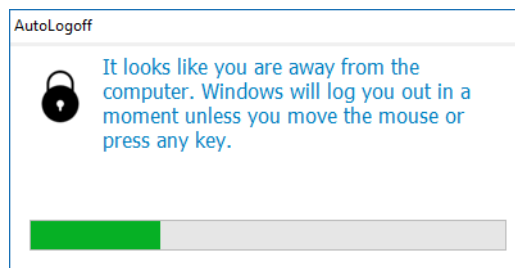# Introduction

AutoLogoff is a compact utility that can perform various user session actions like logoff and restart after it detects an idle computer user. Idle in this case means that no user input is received during a specified amount of time. User input is specifically defined as 'key up', 'mouse button up', 'mouse move' or 'scroll wheel move'. Possible actions are: *logoff, shutdown, restart, standby, lock, disconnect (switch user), disconnect & standby* or *show message*. The message action can be used to warn the user before initiating the logoff or restart action. Optionally temporary user files like the internet browser cache and contents of the temporary folder can be deleted at logoff.

AutoLogoff can also limit the number of simultaneous logins/sessions per user. If a user reaches this limit after logging in, a dialog is displayed. The user can make a choice to continue or logout. Continuing will end the oldest session of the user after a few minutes.

AutoLogoff is especially useful in shared computer environments like schools, libraries and hospitals. Computers stay available for use. It adds a layer of security for users who sometimes forget to logout of Windows. It also cleans up the user profile by deleting unnecessary temporary files that build-up over time. User profiles stay small and manageable (especially important on remote desktop servers).

Contents of the AutoLogoff.zip archive

Config\ADMX (folder)	This folder contains the custom policy template definitions for AutoLogoff (admx/adml files).
Portable\AutoLogoff2.exe	Main program. AutoLogoff2.exe can be run directly from a network share.
Install\AutoLogoff2.msi	Stand-alone file for optional workstation installation.
Portable\AutoLogoff2-64.exe	Main 64-bit program. AutoLogoff2-64.exe can be run directly from a network share.
Install\AutoLogoff2-64.msi	Stand-alone 64-bit file for optional workstation installation.
Config\CopyPolicyDefintions.exe	Copies the admx/adml files to the appropriate location on your pc and network.
Readme.pdf	The file you are reading now.
Agreement.pdf	End user license agreement (EULA)
Config\File\AutoLogoff2.ini	Optional configuration file template
Config\Registry\AutoLogoff2-User.reg	Optional registry template of user configuration settings (HKEY_CURRENT_USER\Software\AutoLogoff2). Use only when NOT using group policies. Import your customized registry-file in your login script for specific users.
Config\Registry\AutoLogoff2-Computer.reg	Optional registry template of computer configuration settings (HKEY_LOCAL_MACHINE\Software\AutoLogoff2). Use only when NOT using group policies. Import your customized registry-file on specific computers that you want to have AutoLogoff enabled for all users.
Config\Registry\AutoLogoff2-Computer -32On64Bit.reg	Same as above. Used when running the 32-bit AutoLogoff version on a computer with a 64-bit OS.

Configuration

AutoLogoff can be controlled by Group Policies OR registry edits OR a configuration file. Path or file names support environment variables. Settings are applied in the following order:

1. %AUTOLOGOFF2_PROGRAM_FOLDER%\AutoLogoff2.ini if it exists
2. %LOCAL_APP_DATA%\AutoLogoff2\AutoLogoff2.ini if it exists
3. HKEY_LOCAL_MACHINE\Software\AutoLogoff2 if it exists
4. HKEY_CURRENT_USER\Software\AutoLogoff2 if it exists
5. Computer AutoLogoff group policy if configured
6. User AutoLogoff group policy if configured

The policy settings can be found at Computer (or User) Configuration/Administrative Templates/AutoLogoff2 .

General

Title	Registry Value	Description
Cleanup temporary user files at logoff	Cleanup	Cleanup temporary user profile files when logging off.
Force disconnect	ForceDisconnect	Force Disconnect makes the manual Lock Desktop command (WIN+L) behave like the Switch User command. The result is that the Windows username/password login dialog is displayed when a session is locked.
Force quit	ForceQuit	Force Quit is strongly recommended (please be aware that data loss can occur if an open document is not saved yet). If not set, a blocking program or lock screen can prevent AutoLogoff from logging off the inactive user. Force Quit will also be applied to a normal logoff initiated by the user.
License	License	The license key has the following format: [company name;domain;number of licenses;end date yymmdd;calculated hash value]

Idle Actions

Define what action(s) to perform after a user has been idle for the specified number of minutes. The restart action will restart the computer if only one user is using the computer. If multiple users are logged in, the idle user will be logged out.

Title	Registry Value	Description
Do not check for inactivity when a full screen video is playing	IgnoreFullScreen	Prevents logging off when watching a long video.
Enable kiosk mode	KioskMode	Kiosk Mode is useful for a Windows configuration that automatically logins and is used as a public information terminal. AutoLogoff will start checking 'idleness' only after the first input is received since the user session started. This prevents the system from continuously logging out and in when no-one is using the system.
Include Injected Input	IncludeInjectedInput	By default AutoLogoff will filter out 'injected' user input (fake mouse and keyboard input) so it will not be tricked by utilities that prevents screen savers and sleep mode ('caffineate'). If this causes issues (ie select remote access software), you can let AutoLogoff treat injected input as 'real' input by enabling this setting.
Idle actions	EnableIdleActions IdleTime1 IdleAction1	Perform the specified action after the user has been idle for the specified number of minutes.

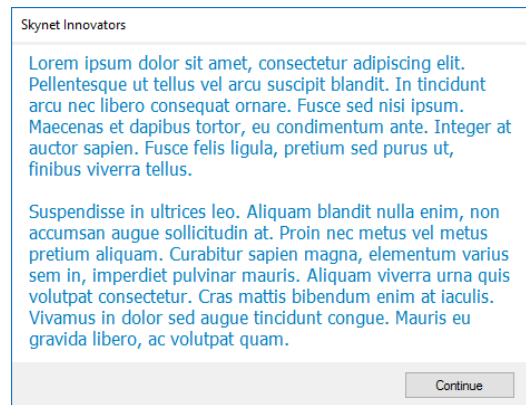|	IdleTime2 IdleAction2 IdleTime3 IdleAction3 IdleTime4 IdleAction4 (Nothing = 0, Show Message = 1, Disconnect = 2, Disconnect & Standby = 3, Lock = 4, Logoff = 5, Restart = 6, Shutdown = 7, Standby = 8)	Configuration Example: Idle Time 1: 20 Idle Action 1: Show Message Idle Time 2: 22 Idle Action 2: Lock Idle Time 3: 30 Idle Action 3: Logoff
Idle action enforcement period	EnableIdleActionPeriod StartTime EndTime	You can optionally specify that Idle Actions should run in a limited time period only with Start Time and End Time. I.e. 9:00 17:00 or 17:00 9:00 (the next day).
Idle message	IdleMessage	Define the message shown to the user when action 'Show Message' is configured.

Notifications

Enabling this policy shows a message/disclaimer to the user upon logon or after the text file is modified.

Title	Registry Value	Description
Show notification message	EnableNotificationMessage NotificationMessageFilePath ContinueButtonText	If the notification message file path is specified, the contents of this file will be shown to the user at logon or within 5 minutes after the contents of this file have been modified. The file is expected to be UTF-8 encoded.

Rest Breaks

Remind your computer users to task a break occasionally in a non-intrusive way.

| Title	Registry Value	Description
Show rest break reminders	EnableRestBreaks BreakPeriod WorkingPeriod RestBreakMessage	Shows a reminder to take a break for [Rest Break Length in Minutes] to the user when he/she has been using the computer continuously for [Working Period in Minutes] minutes without taking a break for at least the specified number of minutes.

Sessions

Limits the number of computers one user can use simultaneously. When the limit is reached, an informational dialog is displayed at logon with a 60 second countdown timer. Should the user decide to continue his/her oldest session will be closed within 11 minutes.

Title	Registry Value	Description
Session data path	SessionDataPath	Users must have write access to the Session Data Path folder. A session file will be created when a user logs on. This file will be deleted at logoff time. A text file UserEvents.log is created in the Session Data Path folder. This is a tab-separated file containing information about logon and logoff events. A copy of this file can be opened in Excel (Excel locks files).
Session limit	EnableSessionLimit SessionLimit SessionLimitMessage LogoffButtonText ContinueButtonText	Limits the number of computers one user can use simultaneously. When the limit is reached, an informational dialog is displayed with a countdown timer. If the user decides to continue, his/her oldest session will be terminated.

Configuration with Group Policies

To configure AutoLogoff with group policy (recommended) copy the contents of the ADMX folder to the following location on your network: \\%userdnsdomain%\sysvol\%userdnsdomain%\Policies\PolicyDefinitions. A faster way is to run the accompanied CopyPolicyDefinitions.exe. It will do the above for you. If this network folder does not exist yet you can create one by copying the contents of the folder C:\Windows\PolicyDefinitions from a Windows 7+ computer to this network location.
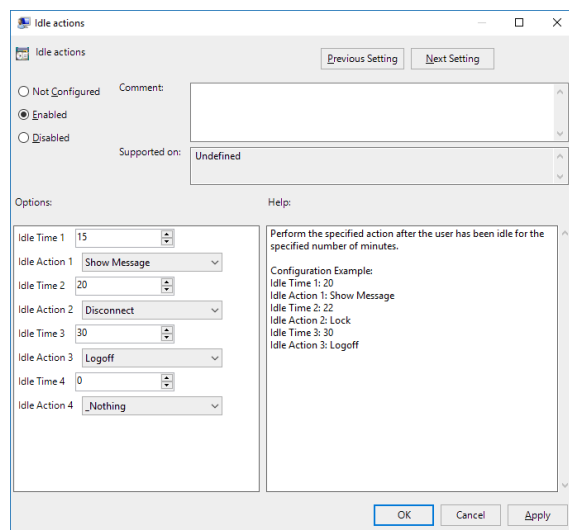
Next use the Group Policy Management console on Windows Vista, 7, 8, 10, Windows Server 2008 or 2012 to configure settings. You can use the Remote Server Administration Tools for this: http://www.microsoft.com/en-us/download/details.aspx?id=7887 (Windows 7) or https://www.microsoft.com/en-us/download/details.aspx?id=45520 (Windows 10) . It can take some time for computers to apply new group policy settings. You can use the build-in Windows command gpupdate to force reapplying changed group policies.

Configuration with registry or configuration file

If you are NOT using group policies, you can use the accompanied AutoLogoff2-User.reg or AutoLogoff2-Computer.reg registry files as template for configuration. Import these registry settings with a command like *reg import \\server1\share\AutoLogoff.reg* in your login script when using user specific settings OR double click to import as administrator when using computer specific settings. You can open the example files in a text editor to see the settings (calc.exe in programmer mode will help with dec<>hex conversion). We suggest to import the file into the registry, customize the settings with regedit.exe and export the settings to a new registry-file.

Probably easier is to use the *AutoLogoff2.ini* text configuration file (utf-8 encoded). Edit it to your liking (notepad++ is a good free editor). When don, copy it to the folder where AutoLogoff2.exe is located to apply it to all users of the computer OR copy it to %appdata%\AutoLogoff2 to apply it to the current user only.

Running AutoLogoff on your clients

To run AutoLogoff2.exe on the workstations one option is to edit your logon script to include a reference to AutoLogoff2.exe. We advise to use UNC notation (*server\share\AutoLogoff2.exe*). The tool does not need administrator rights. If you want to install and run the program locally instead you must run AutoLogoff2.msi once on each computer as administrator or deploy it using group policy software deployment. This will install AutoLogoff2.exe to C:\Windows and add an 'all user run entry' to the Windows registry so that the program will start at each user login.

When no valid license is entered, the program shows a license dialog every 16 minutes. This happens only when AutoLogoff is configured for the computer.

You can run the 32-bit version on both 32-bit and 64-bit Windows. You may choose to use the 64-bit version on 64-bit Windows. There is no difference in functionality between the two. It is developed and delivered to show that AutoLogoff is 'futureproof'.

Logging

AutoLogoff keeps a local log file in *%localappdata%\AutoLogoff2\Session.log* . This log file contains information about session status change events.

If the Session Data Path is specified, a central log file will be created named UserEvents.log that contains logon and logoff information. The format is [date time<tab>type<tab>computer<tab>user].

Example Configuration

1. Copy the AutoLogoff ADMX files to the central ADMX store:
   \\%userdnsdomain%\sysvol\%userdnsdomain%\Policies\PolicyDefinitions
2. Create an AutoLogoff group policy object in the OU where your users are located (or computers if you want to target all users that logon to those computers)
3. Configure the group policies (example):
   a. General/Cleanup temporary user files at logoff: Enabled
   b. General/Force quit: Enabled (important!)
   c. Idle Actions/Idle message: Enter a message to display as warning to end users
   d. Idle Actions/Idle actions: Enabled
       i. Idle Time 1: 20 (user is inactive for 20 minutes)
       ii. Idle Action 1: Show Message (will show the configured message above)
       iii. Idle Time 2: 22 (user has been inactive for 22 minutes)
       iv. Idle Action 2: Disconnect
       v. Idle Time 3: 30
       vi. Idle Action 3: Logoff
4. Optionally enable Notifications/Show notification message to display a 'welcome message' to the end user
   a. Enter UNC path (\\server\share\message.txt)
5. Install or run AutoLogoff2.exe on client workstations by either installing it locally with AutoLogoff2.msi (can also be distributed with Group Policy Software Distribution) OR simple copy it to the NETLOGON share and run it via the users logon script by adding a command: *start "* *\\%userdnsdomain%\netlogon\AutoLogoff2.exe"*